ROYAL MELBOURNE INSTITUTE OF TECHNOLOGY

CENTENARY INTERNATIONAL CONFERENCE

MELBOURNE

14 MAY 1987

SESSION 3 INFORMATION MANAGEMENT AND MISMANAGEMENT

"THE LAW AND INFORMATION"

ROYAL MELBOURNE INSTITUTE OF TECHNOLOGY

CENTENARY INTERNATIONAL CONFERENCE
MELBOURNE

14 MAY 1987

SESSION 3 INFORMATION MANAGEMENT AND MISMANAGEMENT

THE LAW AND INFORMATION

The Hon. Justice M.D. Kirby, CMG*

DATA PROTECTION LAWS

Well may you ask how a Judge becomes involved in a session of this kind, in a conference on this topic. When I was appointed Chairman of the Australian Law Reform Commission, I expected to be busying myself in familiar territory, such as the Statute of Limitations and the Rule against Perpetuties. Instead, that Commission was put to work by successive Attorneys-General in areas of the law involving its interface with technology: the law of human tissue transplantation; the law of privacy. The latter project took me to the OECD in Paris. I there became Chairman of an Expert Group working on the rules that should govern the protection of privacy in transborder data flows. The Committee prepared guidelines.[1] Those guidelines have influenced the development of domestic laws in many of the 24 countries of the OECD. In this way, an international body contributed to diminishing inefficient differences in laws operating on a common technology.

The focus of this session is the management and mismanagement of information. That was also the focus of the attention of the OECD Committee, whose recommendations in due course were adopted by the OECD Council. Stimulated by developments in the law in a number of countries and by proposals in a number of international bodies, the OECD established principles which were designed to secure harmony between a number of competing interests. Most important amongst these were the interests in the protection of individual privacy, notwithstanding the exponential growth in the flow of data about all of us and the protection of the free flow of data, unimpeded by inefficient rules.

As a recent Canadian report suggests, there is an inherent tension between the right to privacy and the right to know. This report is titled "Open and Shut".[2] What the law has to do is to define with appropriate precision the areas to be "shut" whilst maintaining a general bias in favour of that openness which is important for political and economic rights.

The Australian Law Reform Commission reported on a package of laws for the protection of privacy in those areas under Federal regulation. The report has not yet been implemented. Although there are many in our society who speak up for privacy invasions - especially by telephonic interception and a universal identity card - there is no effective legal framework to speak up for the protection of the information penumbra relating to individuals which may be called the "privacy" claim. The recently defeated Australia Card legislation did contain provision for a data protection agency. But its mandate was strictly limited to protection in

connection with the Australia Card data. It had no wider mission. And it fell with the defeat of the Australia Card Bill.

This being the case, despite the rapid growth of information technology and the exponential growth of access to personal data, no effective legislative protections have yet been established in Australia. In this regard, Australia lags behind many other OECD countries. In Europe, where the misuse of personal data by the Gestapo is still fresh in mind, Data Protection Acts have been passed. They generally have a heavy emphasis on bureaucracy, licensing and Government regulation of data banks collecting personal data. The Australian Law Reform Commission proposed a more low key and cost effective mechanism. In default of its proposals, the protection of the privacy interest in personal data is, for the moment, left very much to the initiatives and consciences of information managers themselves.

Pending the enactment of laws giving legal protection to privacy interests (and even perhaps after such laws are enacted) much depends upon the attitudes of information managers of what may be called "fair practices" concerning personal data. The Australian Law Reform Commission principles in this regard are attached to my paper, as a schedule. They adopt a chronological sequence, as do the earlier OECD Guidelines. They trace the flow of personal information through collection, storage, use and disclosure. The general object can be seen to be the limitation in the collection of unnecessary personal data, and its fair use as it moves through the data system. As well, the principles adopt the vital provision (which exists in all information privacy rules adopted so far).

This is the right of the individual, normally (with expections being only those spelt out by law) to have access to data about himself or herself. The object in these controls, whether in the movement of the data or in the right of access is simple. It is to keep ultimate control about the information penumbra concerning an individual in the hands of that individual so that he or she can determine how others in the world perceive him or her from the data penumbra. In the future more and more decisions will be made by Government, management and indeed all of us based upon this personal data penumbra. That is why the core principle of fair information practices universally adopted by privacy protection laws accepts the right of the individual to know and have some control over this extension of personality provided by the circulating personal data.

There are already provisions in Australia law which give the individual rights of access to personal records and rights of correction, deletion or annotation in certain circumstances. The most obvious are to be found in freedom of information laws which exist at the Federal level and in Victoria. Unfortunately, these laws, though also enacted in many overseas jurisdictions, have not spread to the other Australian states.

PRIVACY LAWS AND SIR HUMPHREY

Most of you will watch "Yes Minister". That paragon of the civil service, Sir Humphrey Applebee shows how cleverly the determined administrator can hold up progress and manipulate well intentioned reforms to an entirely different direction. I do not say that this could possibly happen in Australia. But it will not have escaped attention that, despite many political promises of freedom of information laws, these beneficial

provisions have not yet been enacted for most of the public service of Australia. Furthermore, effective laws for the protection of privacy have not yet been enacted at all. The only recent proposal in connection with privacy protection came not in a general Federal law for the implementation of the Law Reform Commission's report. It was contained in proposals, originating from the bosum of the bureaucracy in Canberra. These were the proposals to adopt a national identity card. The privacy provisions were not suggested for the general protection of the citizen's interest in fair data practives, for the implementation of the OECD Guidelines or the Law Reform Commission report or to follow the laws of so many other Western countries to preserve privacy interests. Instead, the proposals for data protection were added as a "sweetner" to the ID proposals. Little wonder that the suggestion attracted so many critics and has now been defeated for the second time by the Senate.

We may be witnessing Sir Humphrey's "fourth rule". You will recollect that this is to delay implementation of a report proposal until either everyone has forgotten it or the problem which it addressed has changed requiring an entirely new investigtion. One of the difficulties of developing laws to govern information movements is the rapid advance in the technology of information. The technological advances in the analysis of data by modern information technology may be such that use can be made of data (collected for an entirely neutral purpose) to focus in on an identified individual. The simplest example will be material in newspapers. This material may have been collected for news purposes. In the past, the reference to

an individual would probably have been lost entirely in the massive quantity of news material. But by the developing technology of free text retrieval, data which was not specifically collected in connection with the later identified data subject, may with speed and economy be retrieved from what would otherwise have been its safe burial place.[4] Some of the principles both in the OECD Guidelines and in the Law Reform Commission report will in due course need to be reworked in the light of the diminished importance of the one to one relationship between data and a data subject. To some extent the Law Reform Commission anticipated this change. It was for this reason that it suggested a very flexible institutional machinery which could adapt with changing technology.

OTHER CONCERNS OF MANAGEMENT

The institution of fair information practices to protect data having personal identifiers is only one of the concerns of the information manager. The range of legal concerns which have been identified as affecting the flow of data, is extremely wide. It relates to such matters as -

* changes in intellectual property law (trade marks, copyright and patent law) to move from protection of the medium of information to possible protection of the information itself.
* changes in contract law to reflect the effecting of obligations by electronic messages without written agreements and frequently at very great speed.
* the provision of effective criminal laws to deal with anti-social conduct having connection with a number of jurisdictions in transborder data flows.

* the provision of an effective regime of private international law to determine the choice of law which will apply to a transaction having connection with a number of States or even a number of countries.
* the determination of criminal laws to deal with the growing problem of "computer fraud" and theft of information.

The fundamental problem, demonstrated by the tardy response to the Law Reform Commission's Report on Privacy, is an institutional one. Problems are being presented to our democratic institutions which are at once complex and urgent. They require effective inter-related responses. But the responses must be flexible not only because of the economics of legal regulation but also because of the rapid changes in the technology that gives rises to the need for protection in the first place.

It has to be said that there are few bodies in the international field which are working on the multi-faceted and complex issues presented by advances in technology. The OECD has done some valuable work but more problems are presenting than solutions are being offered. On the national scene, the lack of a coordinated approach to the provision of informed, cost effective and accessible laws for information managers must be a source of growing concern. Unless lawyers and parliaments can work out the legal responses required to deal with the problems posed by changes in information technology, we will see the creation of an ever increasing area of important human activity which is not subject to relevant legal regulation or the effective operation of the rule of law. It

will not be a true legal vacuum. The common law sees to this. Judges will always derive rules from analogous reasoning derived from general legal principles. But it will be much better for our information managers and for our society if the rules governing the use of information technology were developed in a logical and informed way and promptly enacted by Parliament. That was the object of the Law Reform Commission. Unfortunately, it is an object which, in the field of privacy, has not yet been successfully accomplished. The break down in the inter action between complex new technology and our democratic law making institutions should be a source of concern to all democrats in Australia. At stake is nothing less than the survival of parliamentary government in the age of mature technology.

FOOTNOTES

* President, Court of Appeal, Supreme Court, Sydney. Former Chairman of the OECD Expert Group on Transborder Data Barriers and the Protection of Privacy (1978-80); Chairman, Australian Law Reform Commission (1975-74); Governor, International Council for the Computer Communication (1985-).

1. OECD, Guidelines on the Protection of Privacy and Transborder Flow of Personal Data, OECD, Paris, 1981.
2. Canada, House of Commons, Report of the Standing Committee on Justice and Solicitor-General on the Review of the Access to Information Act and the Privacy Act, Open and Shut: Enhancing the Right to Know and the Right to Privacy, 1987.
3. A. Marshall, "The 'Australia Card' - Survey of the Privacy Problems Arising from the Proposed Introduction of an Australian Identity Card" (1986) 2 Journal of Law and Information Science 111.
4. P. Thorne and J. Thom, "Privacy Principles - Tacit Assumptions under Threat" (1986) 2 Journal of Law and Information Science 68. See also G. Greenleaf and R. Clarke, "A Critique of the Australian Law Reform Commission's Information Privacy Proposals" (1986) 2 Journal of Law and Information Science 83.

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:

   a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;

   b) "personal data" means any information relating to an identified or identifiable individual (data subject);

   c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

   a) the application, to different catagories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

   b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

   c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

   a) as few as possible, and

   b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO
BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identify and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

i) within a reasonable time;

ii) at a charge, if any, that is not excessive;

iii) in a reasonable manner; and

iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs *(a)* and *(b)* is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.